optimal control + game

min max Ham(u,v)

Differential Security Game in Heterogeneous Device-to-Device Offloading Network Under Epidemic Risks

Letian Zhang, *Student Member, IEEE* and Jie Xu, *Member, IEEE*

***Abstract*—Cooperative computation among peer mobile devices via device-to-device (D2D) links, a.k.a. D2D offloading, is a promising technology to enhance mobile computing performance and reduce core wireless network traffic. However, D2D offloading also creates new security risks as malware can relatively easily compromise mobile devices participating in D2D offloading and propagate across the entire network. In this article, we build an epidemic model to understand the malware propagation process in the D2D offloading-enabled mobile network where devices have heterogeneous computation demand and new devices can enter the system over time. This model also allows mobile devices to intentionally enter a "non-cooperative" state as a preventive defense strategy to thwart malware propagation. We prove a thresholding result of the malware propagation similar to that in classic epidemic models under given static defender (i.e. the network operator) and attacker strategies. We further model the strategic interaction between the defender and the attacker as a zero-sum differential game. The existence of a saddle-point equilibrium is proved, and the optimal dynamic defense and attack strategies are derived based on the Pontryagin's maximum principle, which are proven to be a bang-bang control strategy. Simulation results validate the proposed model and show that the dynamic optimal strategies significantly improve the system utility compared with baseline strategies.**

***Index Terms*—D2D offloading, heterogeneous network, differential game, malware propagation.**

I. Introduction

MOBILE applications, such as virtual/augmented reality, cognitive assistance and mobile gaming, are becoming increasingly computation-expensive, latency-sensitive and data-hungry. This poses new challenges on the current cellular-cloud architecture where mobile devices offload complex computation tasks and associated data to the cloud residing in remote data centers via the cellular network [1]. On the one hand, the large and unpredictable round trip delay between the end device and the remote cloud easily renders latency-sensitive mobile application unusable. On the other hand, the ever-growing number of mobile devices generate a large volume of sensory data that easily exceeds the network capacity, overloading the network and degrading the quality of experience of mobile users. To overcome these drawbacks, device-to-device (D2D) communication is leveraged to enable collaborative computation among nearby peer mobile devices, thereby fully unleashing the potential of mobile devices' computation power [2]. This technique, known as D2D offloading, benefits from the fact that mobile devices in close proximity can establish direct wireless communication link over the licensed spectrum (*inband*) or unlicensed spectrum (*outband*) while bypassing the cellular infrastructure such as the base stations. A complex computation task then can be divided into smaller sub-tasks and offloaded to nearby mobile devices with spare computation resources via the D2D link, and once are finished processing, returned to the original requester.

While D2D offloading produces significant benefits in terms of improved communication and computation efficiency, it also creates new security risks to mobile devices as well as the overall system as it relies on ordinary mobile devices whose security protection is much weaker than the operator network and the cloud [3]. Specifically, an attacker can launch proximity-based attacks: malicious codes can be disguised as or embedded into complex computation tasks in order to compromise mobile devices that provide the computation service. Although computation tasks are often run in an isolated virtualized environment such as a sandbox on the peer mobile device, the attacker can still exploit various side channels (e.g. shared memory) to compromise the mobile device [4]. What is worse, compromised mobile devices can become new sources of attack as they interact with non-compromised mobile devices in D2D offloading in the future, thereby spreading the malware/attack over the entire network [5]. Therefore, mobile devices face epidemic security risks when participating in D2D offloading.

In this paper, we aim to answer two fundamental questions in D2D offloading under such epidemic security risks: (1) How does malware propagate in a D2D offloading network? (2) How to design optimal defense strategies against such epidemic attacks? To this end, we build an epidemic model tailored to the D2D offloading system, formulate the attack-defense interaction as a differential game and derive the optimal dynamic defense strategy to protect the D2D offloading network. The main contributions of this paper are as follows.

Manuscript received July 22, 2019; revised September 25, 2019; accepted November 7, 2019. Date of publication November 22, 2019; date of current version September 2, 2020. This work was supported by the Army Research Office under Grant W911NF-18-1-0343. Recommended for acceptance by G. Xiao. *(Corresponding author: Letian Zhang.)*

The authors are with the Department of Electrical and Computer Engineering, University of Miami5452, Coral Gables, FL 33124 USA (e-mail: lxz437@miami.edu; jiexu@miami.edu).

This article has supplementary downloadable material available at http://ieeexplore.ieee.org, provided by the authors.

Digital Object Identifier 10.1109/TNSE.2019.2955036

1) To model epidemic risks in D2D offloading, we extend classic epidemic models and tailor it to the D2D offloading system. The model captures three salient features: (1) the network is dynamic and new mobile devices can enter the system; (2) mobile devices are heterogeneous in terms of computation power and demand; (3) mobile devices have the option to *decline* a computation offloading request. The last feature is particularly interesting as intentionally declining cooperation (i.e. providing offloading service) is in fact a type of preventive defense strategy to thwart malware propagation, which is very different from conventional remedial strategies such as security software patching.
2) We perform invariant system state analysis under static attack and defense strategies and show the existence of a phase-change effect depending on the strategy parameters: the epidemic dies out in the long run if and only if a function value of strategy parameters is below a threshold (see the specific function form in Section III). This result resembles the phase-change effect in classic epidemic models and is important as it provides guidelines for designing defense strategies against static attack strategies.
3) We further investigate the optimal defense strategy (e.g. patching and choosing to be non-cooperative) to maximize the total system utility, taking into account various security costs. However, this is not a simple optimization problem because both the defender (i.e. the network operator) and the attacker are strategic but have oppositive objectives. To model the dynamic strategic interactions between the defender and the attacker, we formulate a zero-sum differential game. The existence of the Nash equilibrium (specifically the saddle-point equilibrium) is proved, and the optimal dynamic strategies are then derived using the Pontryagin's maximum principle [6], which are shown to have a bang-bang property. optimization game NE; 最优策略的存在性
4) We perform extensive system-level simulations for a wide variety of practical network settings (e.g. wireless transmission range and user mobility). The results validate our analysis and demonstrate the effectiveness of the derived optimal defense strategy.

The rest of this paper is organized as follows. Section II reviews the related work. Section III describes the system model. Section IV formulates the malware defense problem as a dynamic game and derives the optimal strategies. Section V shows numerical results followed by conclusions in Section VI.

II. Related Work

Recent research on the D2D offloading focuses on the themes of resource sharing and cooperative computing [7]–[9]. In [7], [8], authors exploit the non-causal information on the helper-CPU and propose a computation offloading strategy to minimize user-energy consumption. In [9], a cooperation policy optimized using Lyapunov optimization theory is developed to control the Peer-to-Peer offloading in D2D communication systems. However, in our paper, we focus on studying the dynamic attack-defense strategy when malware propagates in D2D network.

Various epidemic models have been proposed in the literature to study virus propagation in human societies and computer networks (see comprehensive surveys in [10], [11]). However, conventional epidemic models are not appropriate for our model, because they do not capture the feature of non-cooperation in D2D offloading networks. Note that non-cooperation is different from quarantine in some epidemic models [12]. This is because while quarantine isolates infected individuals, non-cooperation is a preventative strategy for uninfected individuals.

There are two major kinds of methods to control the epidemics [13]. The first kind focuses on modifying the network structure to prevent the epidemic from breaking out. For example, in [14], certain nodes are removed from the network and therefore unable to contact with the epidemic. However, in these works, the current states of the network are not taken into consideration and the exact information of the entire graph and parameters of the network is required.

The second kind addresses these issues and different epidemic control methods have been proposed as we discuss next. In [15], a vaccination strategy is developed based on impulsive control for controlling the epidemic spread of disease. In [16], authors quantify the maximum damage on the system by considering the most vicious attacks from the attacker's point of view. In [17], authors consider a rumor propagation model with latent period and design strategies in an emergency event. These works, however, critically depend on the homogeneous mixing assumption, which means that all pairs of nodes are the same and uniformly distributed in the network. Hence, the same optimal control strategy can be applied to all network nodes.

Recently, many authors have investigated optimal control for propagation models on heterogeneous networks. In [12], [18], the network structure is divided into several groups by the degree of nodes, and authors explore the influence of the heterogeneous structure on the optimal epidemic control. Similar techniques are also used in the study of information dissemination over the social network. In [19], a continuous and a pulse control are proposed to analyze the rumor spreading dynamics in degree heterogeneous mobile social networks. In [20], an optimal resource allocation is proposed to maximize the information dissemination in scale-free social networks based on Erdos-Rényi degree distribution. As D2D offloading networks do not have a fixed topology and fixed set of neighbors, we model node heterogeneity by its computation demand. More importantly, the aforementioned works only consider how to control the epidemic propagation or how to maximize the information dissemination, but the strategic interaction between the defender and the attacker is not studied.

Game theory can be used to characterize the interactions between the defender and the attacker and has been applied to study the epidemic prevalence and control strategies. In [21], nonzero-sum discounted stochastic games are used to formulate

a robust optimization model for realizing intrusion detection. The repeated game used in [22] achieves vaccination decisions to optimally control malware diffusion. The evolutionary Poisson game constructed in [23] reflects interactions between heterogeneous agents and malware in order to realize epidemic protection over heterogeneous networks. However, these works consider fixed interaction graphs of the nodes, which are not appropriate for the varying topology of the D2D network. A zero-sum dynamic game model is developed to investigate the strategies of both the defender and the attacker on malware propagation in mobile wireless networks [24], where mobile devices have the same type and are always cooperative. The most related work to our paper is perhaps [25]. In [25], a sleeping state is introduced in the epidemic model as sensor nodes can enter the sleeping mode to save energy. Compared with this work, our model considers the new mobile device arrival process and introduces a non-cooperative state in the epidemic model to proactively thwart malware propagation. Moreover, our D2D network is dynamic and heterogeneous instead of static and homogeneous. Our prior work [26] designs incentives for mobile devices to participate in D2D offloading under epidemic security risks, where the attack strategy is considered as fixed and given. In the current paper, we study the optimal dynamic strategies of both the defender and the attacker.

III. System Model

A. D2D Offloading Network

We consider a continuous time system and a wireless network where mobile user equipments (UEs) share computation resources via wireless D2D links. We adopt a continuum population model for UEs to capture the large number of UEs in the network. When two UEs m, n move close to each other due to mobility, they enter each others' physical transmission range and hence a D2D link can be built between these two UEs. Suppose UE m has computation tasks that exceed its own computation capacity, then it can send a request to UE n for collaborative processing via the D2D link. Depending on UE n's willingness to share spare computation resources, UE n can decide either to accept this request or decline it. For clarity, we call UE m the *requester* and UE n the *server* in this matched pair. Note that because the UE population is large, there are many such matched requester-server interactions in the network at the same time, and each UE can be a requester when it has excessive computation tasks but can also be a server when it is idle. However, at any particular time t, an individual UE plays only one role.

We consider heterogeneous UEs that differ in their computation demand, depending on their owners' activity patterns. For instance, owners of some UEs may be enthusiastic about mobile gaming and hence, they may have more computation demand than owners of other UEs that mostly only browse the web. To model this heterogeneity, we divide UEs into K types according to the computation demand: UEs have the same type k if they have similar computation demand. To enable analytical tractability, our model makes a stronger assumption: UEs have the same type k if they have the same *expected computation demand rate* d^k following a Poisson process. However, since our model does not restrict the total number K of types, this approximation will be more accurate as K becomes large. When a UE is not a requester, it can be an available server or an unavailable server (which will not receive the request and cannot serve). We denote q as a coefficient representing the probability that a server is available. Let P^k be the rate of receiving an offloading request from an individual type-k UE, which is an increasing function of d^k and q given the UE mobility model and the wireless transmission range. Fig. 1 shows a snapshot of a part of the network at time t. Due to UE mobility, the physical topology of the network is not fixed. As a result, the logical matchings of requesters and servers are also changing over time depending on both the physical topology and the request arrival process.

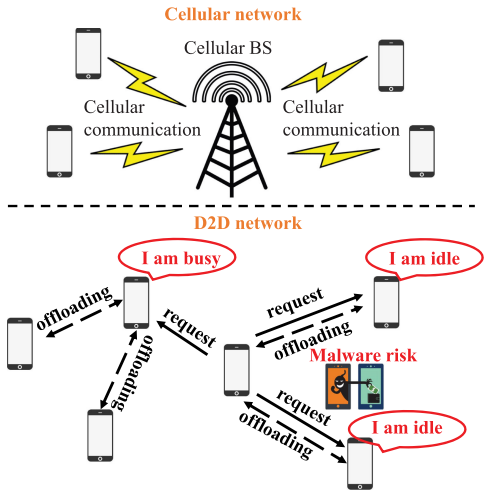


Fig. 1. Snapshot of a portion of D2D network at time t.

In our D2D offloading network, UEs setup D2D links and start D2D communication autonomously with no intervening from the network operators. The network operator has the ability to monitor the security condition of all UEs, install security patches to either prevent normal UEs from known attacks or to cure compromised UEs, and even disable the D2D offloading service when malware spreads widely in D2D network. This is similar to the loosely controlled D2D mode described in [27].

B. Malware Propagation Model

If a server decides to accept the request, then it receives computation tasks offloaded from the requester. However, if the requester is a compromised UE by an attacker, then the attacker can disguise the malware as or embed the malware into a normal task and hence may propagate the attacks to the innocent server UE. This causes the spread of malware over the entire network. To fully describe the system, we build an epidemic model with four basic UE states:

1) *Susceptible (S)* means that UEs are susceptible to malware but have not yet been infected.
2) *Infectious (I)* means that UEs have been contaminated by malware but can still make requests.

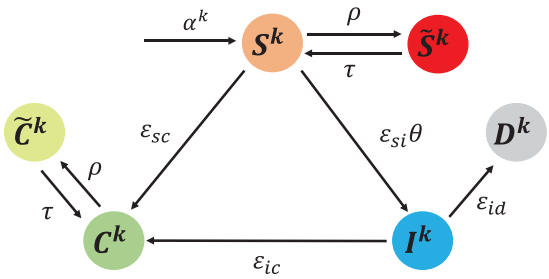


Fig. 2. State transition of a type-k UE.

3) *Cured (C)* means that security patch has been applied to UEs, who then are immune to the malware.
4) *Dead (D)* means UEs are killed by malware, who become dysfunctional and cannot further spread the malware.

We also introduce two more special "non-cooperative" states $\tilde{S}$ and $\tilde{C}$, which mean that the UEs always decline requests when they are susceptible and cured, respectively. UEs can enter these states intentionally when they are reluctant to cooperate or unintentionally when they do not have spare computation resources. We note that a UE in the *Infectious* state will always be cooperative as the purpose of the attacker is to spread the malware as widely as possible. In summary, S, I and C are the *active* states where UEs participate in collaborative computing, whereas $\tilde{S}$, $\tilde{C}$ and D are *inactive* states. Fig. 2 shows the transition between different states. The parameter on the directed link connecting two states represents the rate at which a state transits to the other. These parameters can be categorized into three classes: (1) **Network operator-controlled parameters** $\varepsilon_{sc}, \varepsilon_{ic}, \rho$. For UEs in the *Susceptible* state or the *Infectious* state, the network operator (as the defender) can control the frequency at which security patches are applied to these UEs and hence ε_{sc} and ε_{ic} are defender-controlled parameters. The network operator can also choose to reduce the cooperation rate and hence ρ is controlled by the defender. (2) **Malware-controlled parameters** ε_{si}, ε_{id}. For UEs in the *Infectious* state, the attacker can choose to kill the UE and make it dysfunctional at a certain rate ε_{id}. However, for UEs in the susceptible state to enter the infectious state, it depends on not only the strength of the malware (represented by ε_{si}) but also the rate at which a UE interacts and cooperates with an already compromised UE (represented by θ). While the former is an attack strategy, the latter is a result of the system dynamics depending on both the defense and the attack strategies. This makes the decision problem of the attacker and the defender intricately coupled. (3) **Exogenous parameters** $\tau, \alpha^k, \forall k$. α^k is the new UE arrival rate of type-k UEs. In this paper we treat τ, which is the return rate from "non-cooperative" states (i.e. $\tilde{S}$ and $\tilde{C}$), as an exogenous parameter for mathematical simplicity. This is because by tuning ρ alone can already control the expected time that a UE is in the "non-cooperative" state.

Without loss of generality, we assume that all control parameters are bounded in [0,1]. The upper bound indicates the maximum capability of the attacker and the defender. Let $S^k(t)$, $I^k(t)$, $C^k(t)$, $D^k(t)$, $\tilde{S}^k(t)$ and $\tilde{C}^k(t)$ be the population of type-k UEs for corresponding states at time t. Then the system dynamics can be fully characterized by the following set of differential equations: for each type k,

这样的说法 似乎更合理

$$\begin{aligned}
\frac{dS^k(t)}{dt} &= \alpha^k + \tau\tilde{S}^k(t) - (\rho + \varepsilon_{si}\theta(t) + \varepsilon_{sc})S^k(t) \\
\frac{d\tilde{S}^k(t)}{dt} &= \rho S^k(t) - \tau\tilde{S}^k(t) \\
\frac{dI^k(t)}{dt} &= \varepsilon_{si}\theta(t)S^k(t) - (\varepsilon_{ic} + \varepsilon_{id})I^k(t) \\
\frac{dC^k(t)}{dt} &= \varepsilon_{sc}S^k(t) + \varepsilon_{ic}I^k(t) + \tau\tilde{C}^k(t) - \rho C^k(t) \\
\frac{d\tilde{C}^k(t)}{dt} &= \rho C^k(t) - \tau\tilde{C}^k(t) \\
\frac{dD^k(t)}{dt} &= \varepsilon_{id}I^k(t)
\end{aligned} \tag{1}$$

即相遇// 不是要分类别吗？
Pk Ik(t)就可以了吧？

where $\theta(t) = \sum_{k=1}^{K} P^k I^k(t)$ is the rate at which a susceptible UE serves an infectious UE. This term couples different types of UE together. Note that while the offloading request rate P^k, $\forall k$ is constant, $I^k(t)$ changes over time. We assume that initially there are a positive population of infectious UEs, namely $I^k(0) > 0, \forall k$, due as initial attacks; otherwise, there will be no malware propagation in the network.

C. Invariant States Under Given Static Strategies

Before we proceed to study the strategic interaction between the defender and the attacker, we first present a result of a threshold effect under *given static* defense and attack strategies (i.e. given $\varepsilon_{sc}, \varepsilon_{ic}, \rho$ and $\varepsilon_{si}, \varepsilon_{id}$). In Section IV, we will formulate the defender-attacker interaction as a dynamic game, and study the optimal dynamic strategies.

The literature often shows a thresholding effect on epidemic propagation [19], [28]. In our model, a similar thresholding effect is also present in the invariant system state, which is summarized in Theorem 1. In particular, we are interested in characterizing the invariant system state $(S^{k*}, \tilde{S}^{k*}, I^{k*})$ where $S^k(t), \tilde{S}^k(t), I^k(t)$ do not change over time. We note that C^k and $\tilde{C}^k$ cannot be invariant for a non-zero value of ε_{sc}, and D cannot be invariant unless $\varepsilon_{id}^k = 0$ or $I^k = 0$, which is the degenerate case. Therefore, they are not included in the definition of invariant system state, which is common in proving epidemic thresholds in existing works [19], [28].

Theorem 1: In an invariant state $\{(S^{k*}, \tilde{S}^{k*}, I^{k*})\}_{k=1,\ldots,K}$, we have $I^{k*} = 0, \forall k$, if $\lambda \leq 1$, where

$$\lambda \triangleq \frac{\varepsilon_{si}\sum_{k=1}^{K}\alpha^k P^k}{\varepsilon_{sc}(\varepsilon_{ic} + \varepsilon_{id})} \tag{2}$$

Proof: The proof is given in Appendix A. ■

Theorem 1 states that if the system ever enters an invariant state, malware will extinguish if λ is less than a threshold. The intuition behind this result is as follows. When the malware strength (i.e. ε_{si}) is weak, or the security measures (i.e ε_{ic} and ε_{sc}) are strong, or the attacker chooses to kill the infectious

UEs at a high rate (i.e. ε_{id}), then malware propagation becomes harder and hence may extinguish eventually. However, if $\lambda > 1$, the above analysis does not rule out the possibility that I^k can also be 0. Moreover, it does not say anything about stability of the invariant state, i.e., if any small perturbation will cause divergence from the invariant state. In Theorem 2, we answer these questions regarding the stability of the invariant states. For exposition convenience, we let x_0^* denote an invariable state where $I^{k*} = 0, \forall k$, and x_+^* denote an invariable state where $I^{k*} > 0$ for some k.

Theorem 2: (1) If $\lambda \leq 1$, then the invariant state must have $I^{k*} = 0, \forall k$ and this invariant state x_0^* is asymptotically stable.

(2) If $\lambda > 1$, then an invariant state x_+^* (if exists) is asymptotically stable but an invariant state x_0^* (if exists) is not.

Proof: The proof is given in Appendix B ■

IV. Malware Defense as a Dynamic Game

In this section, we model the interaction between the defender and the attacker as a dynamic game. This is a more realistic setting than the fixed static strategies in the invariant state analysis as both the defender and the attacker can change their strategies over time depending on the system states. In this game, the defender chooses the defense strategy $\boldsymbol{\phi}(t) = \{\varepsilon_{sc}^k(t), \varepsilon_{ic}^k(t), \rho^k(t)\}_{k=1,\ldots,K}$ for every UE type k at every time $t \in [0, T]$, where T is a given time horizon. Similarly, the attacker chooses its attack strategy $\boldsymbol{\nu}(t) = (\varepsilon_{si}^k(t), \varepsilon_{id}^k(t))_{k=1,\ldots,K}$ for every UE type k at every time $t \in [0, T]$. Let $\boldsymbol{\phi} \triangleq \{\boldsymbol{\phi}(t)\}_{t\in[0,T]}$ and $\boldsymbol{\nu} \triangleq \{\boldsymbol{\nu}(t)\}_{t\in[0,T]}$ denote the complete defense strategy and attack strategy, respectively. These strategies induce a system trajectory $x = \{x(t)\}_{t\in[0,T]}$ where $x(t) \triangleq \{S^k(t), \tilde{S}^k(t), I^k(t), C^k(t), \tilde{C}^k(t), D^k(t)]\}_{k=1,\ldots,K}$.

We consider a system utility function defined as follows

$$\max \quad U(\boldsymbol{\phi}, \boldsymbol{\nu}) = \int_{t=0}^{T} u(x(t), \boldsymbol{\phi}(t), \boldsymbol{\nu}(t))dt \tag{3}$$

where

$$u(x(t), \boldsymbol{\phi}(t), \boldsymbol{\nu}(t)) = \sum_{k=1}^{K}[(\eta_s - \eta_{sc}\varepsilon_{sc}^k(t))S^k(t) + \eta_c C^k(t) - (\eta_i + \eta_{id}\varepsilon_{id}^k(t) + \eta_{ic}\varepsilon_{ic}^k(t))I^k(t)]$$

is the instantaneous utility function. In this utility function, η_s and η_c are the unit benefit for having susceptible and cured UEs in the system, respectively, as they are the contributors to the collaborative computation; η_{sc} and η_{ic} are the unit cost of patching susceptible and cured UEs, respectively; η_i is the unit cost for having infectious UEs in the system (e.g. if the attacker aims to perform stealthy attacks); η_{id} is the unit cost for killing infectious UEs (e.g. if the attacker aims to break down the system). $U(\boldsymbol{\phi}, \boldsymbol{\nu})$ therefore is the total utility over the time horizon $[0, T]$. Note that $S^k(t), C^k(t)$ and $I^k(t)$ are induced by the strategies $\boldsymbol{\phi}$ and $\boldsymbol{\nu}$. Therefore, although $\rho^k(t)$ and $\varepsilon_{si}^k(t)$ do not explicitly appear in the expression of $u(x(t), \boldsymbol{\phi}(t), \boldsymbol{\nu}(t))$, they do influence the system utility implicitly through the system dynamics.

A. Existence of Equilibrium

The malware defense dynamic game is a differential game as it takes place in a system specified by a set of differential equations. We assume that the defender aims to maximize the system utility $U(\boldsymbol{\phi}, \boldsymbol{\nu})$ by choosing $\boldsymbol{\phi}$ while the attacker aims to minimize it by choosing $\boldsymbol{\nu}$, and therefore the game is a zero-sum game. As a result, the Nash equilibrium reduces to a saddle-point equilibrium (or minimax point), which is formally defined as follows.

Definition 1. (Saddle-point Equilibrium). A strategy profile $(\boldsymbol{\phi}^*, \boldsymbol{\nu}^*)$ is a saddle-point equilibrium if and only if

$$\boldsymbol{\phi}^* = \arg\max_{\boldsymbol{\phi}} U(\boldsymbol{\phi}, \boldsymbol{\nu}^*) \qquad \boldsymbol{\nu}^* = \arg\min_{\boldsymbol{\nu}} U(\boldsymbol{\phi}^*, \boldsymbol{\nu}) \tag{4}$$

Theorem 3: There exists a saddle-point equilibrium of the malware defense dynamic game.

Proof: The proof is given in Appendix C ■

B. Optimal Dynamic Strategies

In this subsection, we determine the optimal dynamic strategies $\boldsymbol{\phi}^*$ and $\boldsymbol{\nu}^*$. Specifically, we apply the Pontryagin's Maximum Principle [6] to transform the optimal dynamic control problem into an extremal control problem. We first introduce the Pontryagin's Maximum Principle.

Definition 2: (Pontryagins Maximum Principle). Consider a system $\dot{x}(t) = f(x(t), c(t))$ and an admissible control $c(t)$ to maximize the objective function

$$U(c) = \int_{t=0}^{T} u(x(t), c(t))dt. \tag{5}$$

The optimal control must satisfy $c^* = \arg\max_c H(x^*, \omega^*, c)$ where x^* and ω^* are the optimal state trajectory and co-state trajectory, respectively, induced by c^*. Here H is the Hamiltonian function and $\omega = \{w(t)\}_{t\in[0,T]}$ is the co-state function defined as follows

$$\begin{cases} H(x(t), \omega(t), c(t)) = u(x(t), c(t)) + \omega^T(t) f(x(t), c(t)) \\ \dot{x}(t) = \frac{\partial H}{\partial \omega}, \\ \dot{\omega}(t) = -\frac{\partial H}{\partial x} \end{cases}$$

In the considered malware defense dynamic game, the attacker has an opposite objective than the defender. Therefore, we extend the Pontryagin's Maximum Principle to accommodate the malware defense game as follows

game

$$(\boldsymbol{\phi}^*(t), \boldsymbol{\nu}^*(t)) \in \arg\min_{\boldsymbol{\nu}(t)} \max_{\boldsymbol{\phi}(t)} H(x(t), \boldsymbol{\phi}(t), \boldsymbol{\nu}(t), \omega(t)) \tag{6}$$

$$(\boldsymbol{\phi}^*(t), \boldsymbol{\nu}^*(t)) \in \arg\max_{\boldsymbol{\phi}(t)} \min_{\boldsymbol{\nu}(t)} H(x(t), \boldsymbol{\phi}(t), \boldsymbol{\nu}(t), \omega(t)) \tag{7}$$

We define the Hamiltonian function for our malware defense game as follows

$$
\begin{aligned}
H &= u(x(t), \phi(t), \nu(t)) \\
&+ \sum_{k=1}^{K} \omega_s^k [\alpha^k + \tau \tilde{S}^k(t) - (\rho^k + \varepsilon_{si}^k \theta(t) + \varepsilon_{sc}^k) S^k(t)] \\
&+ \sum_{k=1}^{K} \omega_{\tilde{s}}^k [\rho^k S^k(t) - \tau \tilde{S}^k(t)] \\
&+ \sum_{k=1}^{K} \omega_i^k [\varepsilon_{si}^k \theta(t) S^k(t) - (\varepsilon_{ic}^k + \varepsilon_{id}^k) I^k(t)] \\
&+ \sum_{k=1}^{K} \omega_c^k [\varepsilon_{sc}^k S^k(t) + \varepsilon_{ic}^k I^k(t) + \tau \tilde{C}^k(t) - \rho^k C^k(t)] \\
&+ \sum_{k=1}^{K} \omega_{\tilde{c}}^k [\rho^k C^k(t) - \tau \tilde{C}^k(t)] + \sum_{k=1}^{K} \omega_d^k [\varepsilon_{id} I^k(t)] \qquad (8)
\end{aligned}
$$

and the following differential equations determine co-state dynamics

$$
\begin{aligned}
\frac{d\omega_s^k}{dt} &= -\frac{\partial H}{\partial S^k(t)} = (\rho^k + \varepsilon_{si}^k \theta(t) + \varepsilon_{sc}^k)\omega_s^k + \eta_{sc}\varepsilon_{sc}^k - \eta_s \\
&\quad - \rho^k \omega_{\tilde{s}}^k - \varepsilon_{si}^k \theta(t) \omega_i^k - \varepsilon_{sc}^k \omega_c^k \\
\frac{d\omega_{\tilde{s}}^k}{dt} &= -\frac{\partial H}{\partial \tilde{S}^k(t)} = \tau \omega_{\tilde{s}}^k - \tau \omega_s^k \\
\frac{d\omega_i^k}{dt} &= -\frac{\partial H}{\partial I^k(t)} = (\varepsilon_{ic}^k + \varepsilon_{id}^k)\omega_i^k + \sum_{k=1}^{K} \varepsilon_{si}^k P^k S^k(t) \omega_s^k \\
&+ \eta_{id}\varepsilon_{id}^k + \eta_i + \eta_{ic}\varepsilon_{ic}^k - \sum_{k=1}^{K} \varepsilon_{si}^k P^k S^k(t) \omega_i^k - \varepsilon_{ic}^k \omega_c^k - \varepsilon_{id}^k \omega_d^k \\
\frac{d\omega_c^k}{dt} &= -\frac{\partial H}{\partial C^k(t)} = \rho^k \omega_c^k - \rho^k \omega_{\tilde{c}}^k - \eta_c \\
\frac{d\omega_{\tilde{c}}^k}{dt} &= -\frac{\partial H}{\partial \tilde{C}^k(t)} = \tau \omega_{\tilde{c}}^k - \tau \omega_c^k \\
\frac{\omega_d^k}{dt} &= -\frac{\partial H}{\partial D^k(t)} = 0 \qquad (9)
\end{aligned}
$$

with transversality conditions $\omega_s^k(T) = \omega_{\tilde{s}}^k(T) = \omega_i^k(T) = \omega_c^k(T) = \omega_{\tilde{c}}^k(T) = \omega_d^k(T) = 0$. By re-arranging the terms, the Hamiltonian function can be rewritten as

$$
\begin{aligned}
H = \sum_{k=1}^{K} [&\pi^k(t) + \varepsilon_{sc}^k \kappa_{sc}^k(t) + \varepsilon_{ic}^k \kappa_{ic}^k(t) + \rho^k \kappa_\rho^k(t) \\
&+ \varepsilon_{si}^k \kappa_{si}^k(t) + \varepsilon_{id}^k \kappa_{id}^k(t)] \qquad (10)
\end{aligned}
$$

where

$$
\begin{aligned}
\pi^k(t) &= \eta_s S^k(t) - \eta_i I^k(t) + (\omega_s^k \tau - \omega_{\tilde{s}}^k \tau)\tilde{S}^k(t) \\
&\quad + (\omega_c^k \tau - \omega_{\tilde{c}}^k \tau)\tilde{C}^k(t) + \eta_c C^k(t) + \omega_s^k \alpha^k \\
\kappa_{sc}^k(t) &= (\omega_c^k - \eta_{sc} - \omega_s^k) S^k(t) \\
\kappa_{ic}^k(t) &= (\omega_c^k - \eta_{ic} - \omega_i^k) I^k(t) \\
\kappa_\rho^k(t) &= (\omega_{\tilde{s}}^k - \omega_s^k) S^k(t) + (\omega_{\tilde{c}}^k - \omega_c^k) C^k(t) \\
\kappa_{si}^k(t) &= (\omega_i^k \theta(t) - \omega_s^k \theta(t)) S^k(t) \\
\kappa_{id}^k(t) &= (\omega_d^k - \omega_i^k - \eta_{id}) I^k(t)
\end{aligned}
$$

are the switching functions. Thus, based on the state, co-state and switching function dynamics, Theorem 2 characterizes the optimal defense and attack strategies.

Algorithm 1 Bang-bang control.

Input:
1) D2D network system,
2) Model coefficients: α^k, τ, T,
3) Initial state conditions: $S^k(0)$, $\tilde{S}^k(0)$, $I^k(0)$, $C^k(0)$, $\tilde{C}^k(0)$ and $D^k(0)$,
4) Transversality conditions: $\omega_s^k(T) = 0$, $\omega_{\tilde{s}}^k(T) = 0$, $\omega_i^k(T) = 0$, $\omega_c^k(T) = 0$, $\omega_{\tilde{c}}^k(T) = 0$ and $\omega_d^k(T) = 0$,
5) Initial control strategies $\nu(0)$, $\phi(0)$.

Output:
The dynamic optimal strategies of malware and UEs: ν^* and ϕ^*.

for each $t \in (0, T]$ **do**
  Obtain the states $x(t)$ using (1).
  Calculate $\theta(t)$ and substitute it into (9).
  Obtain the co-states $\omega(t)$ using (9).
  Calculate $\kappa_{sc}^k(t), \kappa_{ic}^k(t), \kappa_\rho^k(t), \kappa_{si}^k(t), \kappa_{id}^k(t)$.
  Update $\phi(t)$ and $\nu(t)$ according to Theorem 2.
end for
return(ν^*, ϕ^*)

Theorem 4: The optimal defense strategy is as follows
1) If $\kappa_{sc}^k(t) > 0$, then $\varepsilon_{sc}^k(t) = 1$; otherwise $\varepsilon_{sc}^k(t) = 0$
2) If $\kappa_{ic}^k(t) > 0$, then $\varepsilon_{ic}^k(t) = 1$; otherwise $\varepsilon_{ic}^k(t) = 0$
3) If $\kappa_\rho^k(t) > 0$, then $\rho^k(t) = 1$; otherwise $\rho^k(t) = 0$

The optimal attack strategy is as follows
1) If $\kappa_{si}^k(t) < 0$, then $\varepsilon_{si}^k(t) = 1$; otherwise $\varepsilon_{si}^k(t) = 0$
2) If $\kappa_{id}^k(t) < 0$, then $\varepsilon_{id}^k(t) = 1$; otherwise $\varepsilon_{id}^k(t) = 0$

Proof: Since H is a linear function in the control parameters, the optimal strategies can be easily derived by checking the signs of the coefficients before the control parameters. ■

The above theorem shows that both the defense strategy and the attack strategy are a bang-bang control strategy - they either exert the maximum effort or zero effort. The functions $\kappa_{sc}^k(t)$, $\kappa_{ic}^k(t)$, $\kappa_\rho^k(t)$, $\kappa_{si}^k(t)$ and $\kappa_{id}^k(t)$ are thus called the switching functions. To compute the optimal dynamic optimal strategies, we first initialize $\phi(0)$ and $\nu(0)$ to be 1, which are substituted into the state and co-state dynamics to calculate the switching function values in a future t. Then, based on the switching function values, the optimal strategies $\phi(t)$ and $\nu(t)$ at time t can be derived. This iteration is replicated until the terminal time T. The pseudo-code of the bang-bang control is given in Algorithm 1. Next, we provide a structural result of the optimal strategy derived using Algorithm 1.

Theorem 5: Given T, the optimal defense strategy satisfies:
1) There exists $t_1 \in [0, T)$ such that $\varepsilon_{sc}^k(t) = 0$ for all $t \in (t_1, T]$.
2) There exists $t_2 \in [0, T)$ such that $\varepsilon_{ic}^k(t) = 0$ for all $t \in (t_2, T]$.
3) There exists $t_3 \in [0, T)$ such that $\rho^k(t) = 0$ for all $\in (t_3, T]$.

The optimal attack strategy satisfies:
1) There exists $t_4 \in [0, T)$ such that $\varepsilon_{si}^k(t) = 0$ for all $t \in (t_4, T]$.
2) There exists $t_5 \in [0, T)$ such that $\varepsilon_{id}^k(t) = 1$ for all $t \in (t_5, T]$.

Proof: The switching functions are determined by the co-state functions (9). Thus, from transversality conditions $\omega_s^k(T) = \omega_s^k(T) = \omega_i^k(T) = \omega_c^k(T) = \omega_c^k(T) = \omega_d^k(T) = 0$, we can get $\kappa_{sc}^k(T) = -\eta_{sc}S^k(t) < 0$, $\kappa_{ic}^k(t) = -\eta_{ic}I^k(t) < 0$, $\kappa_\rho^k(t) = 0$, $\kappa_{si}^k(t) = 0$ and $\kappa_{id}^k(t) = -\eta_{id}I^k(t) < 0$. According to Theorem 2, $\varepsilon_{sc}^k(T) = 0$, $\varepsilon_{ic}^k(T) = 0$, $\rho^k(T) = 0$, $\varepsilon_{si}^k(T) = 0$ and $\varepsilon_{id}^k(T) = 1$. If $\kappa_{sc}^k(t)$ has a zero crossing point at T_1 in $(0, T)$, then $t_1 = T_1$. If $\kappa_{sc}^k(t)$ has no zero crossing point in $(0, T)$, $t_1 = 0$. Thus, we can get $\varepsilon_{sc}^k(t) = 0$ for $t_1 < t \leq T$. We can similarly prove all the remaining claims in Theorem 2. ■

From the Theorem 2, the defense strategies will stop after zeros crossing point (i.e. t_1, t_2, t_3), which means that the susceptible UEs return to their normal offloading schedule, and the defender stops to apply security patches. On the other hand, the attack strategies will kill the infectious UEs after t_5. It means that the final attack strategies are to make the system dysfunctional. These behaviors are shown in the optimal dynamic strategies in the next section.

V. Numerical Results

In this section, we show the numerical results of the proposed model and optimal strategies. The simulation setup is as follows. We divide a unit time in the continuous time system into $T_s = 20$ time slots. There are three types of UEs in a square area of size 100×100 with each type having 100 UEs, and UEs' mobility follows the random way-point model [29]. Specifically, when the UE is moving, it moves at a random speed between 0 and $V_{\max}$ per slot in a randomly selected direction.

A. Impact of Transmission Range and Server Availability Probability on P^k

We first study how the computation demand rate d^k of UEs translates to the coefficients P^k in the definition of θ for different types of UEs depending on UE wireless transmission range. In this set of simulations, we set $d^1 = 6, d^2 = 10, d^3 = 14$ for the three types of UEs. Given current positions and realized roles of UEs, non-requesters in the transmission range of a requester are potential servers with probability q and receive an offloading service request from this requester. However, if there is no potential server in the transmission range of a requester, then this requester cannot make offloading requests and hence cannot offload computation workload. We fix $V_{\max} = 5$, $q = 0.8$ and vary R from 1 to 120. Fig. 3 illustrates the estimated P^k under various wireless transmission range R. As can be seen, P^k increases with R because with a wider transmission range, requester UEs have a larger chance of meeting potential server UEs. However, after $R = 100$, P^k becomes stable. This is because the transmission range becomes so large that it is guaranteed that each server can provide offloading service to any requester (although this scenario is less likely to happen in real world). Fig. 3 illustrates the estimated P^k under various server availability probability q. In this case, we fix $R = 10$ and $V_{\max} = 10$. The result shows that P^k increases with q because with larger available server probability q, there are more potential servers to provide offloading service to the requester.

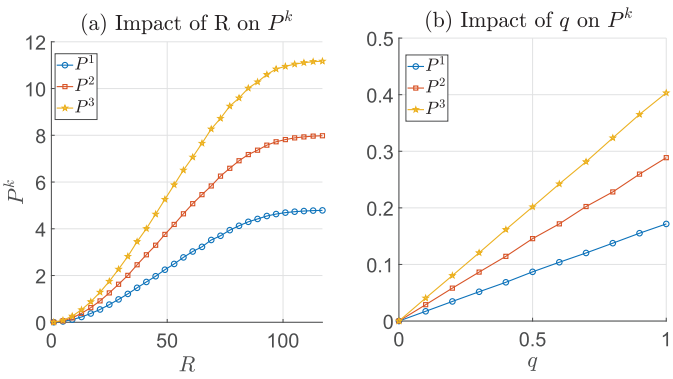


Fig. 3. Impact of transmission range and available server probability on P^k.

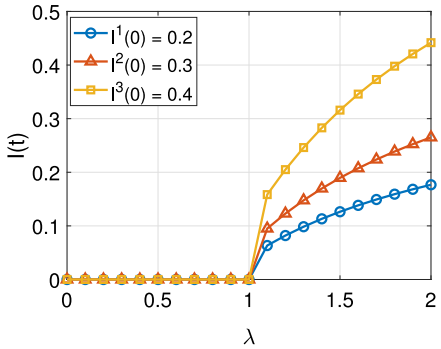


Fig. 4. Impact of λ on final infectious population.

B. Epidemic Threshold

In this subsection, we show the existence of an epidemic threshold predicted in Theorem 1 for fixed static strategies. We set $R = 6$, $V_{\max} = 5$ and $q = 0.8$, so that we can get $P^1 = 0.051$, $P^2 = 0.086$ and $P^3 = 0.121$. We set $\varepsilon_{si} = 1$, $\varepsilon_{id} = 0.05$, $\varepsilon_{ic} = 0.1$, $\rho = 0.1$, and change ε_{sc} to vary λ from 0 to 2. Fig. 4 illustrates converged infectious population under different λ. As can be seen, when $\lambda <= 1$, the final infectious population converges to 0 starting from different initial states whereas $\lambda > 1$ converges to a non-zero value.

C. Optimal Dynamic Strategies

We keep the same network parameter ($R = 6$, $V_{\max} = 5$, $q = 0.8$) and computation demand parameters as above and consider the dynamic defense and attack strategies. Fig. 5 shows the optimal dynamic defense and attack strategies derived according to Theorem 2, and Fig. 6 shows the evolution of the UE population in different states.

We first discuss the defense strategy (ε_{sc}, ε_{ic}, ρ) in this simulation. The defender starts off by exerting the maximum effort in applying security patches to infectious UEs as they are the most dangerous UEs in the system. However, the defender does not initially patch the susceptible UEs. This is because susceptible UEs, although may get compromised, do not propagate malware but patching them incurs additional operational costs. At a later time ($t = 0.5$ for type 1 and $t = 1.0$ for type 3), the defender starts to also patch some susceptible UEs. This is because the epidemics have grown to such a size that the

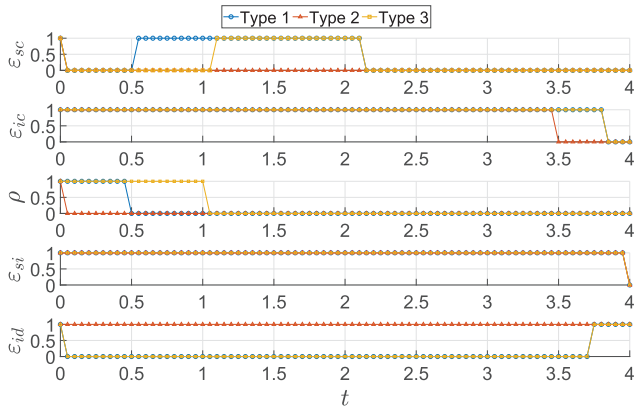


Fig. 5. Optimal dynamic strategies.

defender needs additional remedial measures to control its propagation. As the epidemics die out gradually, the defender stops patching susceptible UEs ($t = 2.1$ for type 1 and type 3). It eventually even stops patching infected UEs because the attacker decides to kill infected UEs. The defender chooses to temporarily minimize cooperation initially by choosing $\rho = 1$ ($t = 0$ to $= 0.5$ for type 1 and $t = 0$ to $t = 1$ for type 3). In this way, existing infected UEs can quickly transit to the cured state by applying security patches on them without further compromising susceptible UEs. When the infected population becomes relatively small, the defender then chooses to maximize cooperation by choosing $\rho = 0$, thereby reaping the maximum benefit of D2D offloading.

Next, we discuss the attack strategy (ε_{si}, ε_{id}). The attacker always exerts the maximum effort to infect susceptible UEs. This is understandable as in our model there is no cost associated with exerting a higher effort by the attacker. Hence, the maximum infection effort leads to the lowest system utility. The attacker does not always exert the maximum effort to kill the infected UEs in type 1 and type 3. This is because killing UEs, although brings some instantaneous benefit to the attacker, reduces the chance of spreading the malware to a wider population. Note however that the attacker always chooses to kill the type-2 infectious UEs. This is because (1) the initial population of type-2 infectious UEs is very large (i.e. $I^2(0) = 0.4$), and (2) the defender gives up defense on type-2 susceptible UEs.

Fig. 6 illustrates the evolution of population over time for different types of UEs. At the beginning, the defender exerts the maximum effort in curing the infectious UEs, so the population of cured UEs greatly increases from $t = 0$ to $t = 2$. The population of susceptible UEs initially decreases as a result of the malware attack but begins to recover at $t = 2$ because the defense strategy successfully restrains the malware propagation. We also notice that the defender did not apply security patching to type-2 susceptible UEs. This is because the population of these UEs did not decrease dramatically at the beginning.

D. Mobility Models and Interaction

Our analytical results are derived based on the assumption of random way-point model, namely UEs have equal probability of meeting another UE. This assumption well captures the scenario where UEs can freely move in the entire area. In this set of simulations, we investigate the cases where UEs move in two different mobility models and the accuracy of our theoretical model. Specifically, we simulate the malware propagation under the dynamic control strategies derived according to Theorem 4 (which is the same as in the previous subsection) for three mobility scenarios.

Case 1: UEs use random way-point model (RWP) in entire area of size 100×100.

Case 2: UEs use mobility model with geographic restriction (GR) [30] in a local area of size 5×5.

Case 3: UEs use Gauss-Markov mobility model (GM) [30] in entire area of size 100×100.

We run the simulation 50 times and average the results, which are reported in Fig. 7. The solid lines are obtained by calculation based on our model; the circle-marked dotted lines are obtained by simulation of Case 1; the triangle-marked dotted lines are obtained by simulation of Case 2; the star-marked dotted lines are obtained by simulation of Case 3. As we can see, the population changes of RWP and GM closely matches our theoretical analysis, demonstrating the effectiveness of our model for scenarios where UEs can freely move in the entire area. When UE mobility is confined in a local area, the simulation shows a gap with our model. In particular, the population of susceptible UEs decreases more slowly while the population of infectious UEs decreases more quickly as the localized interaction slows down the propagation process.

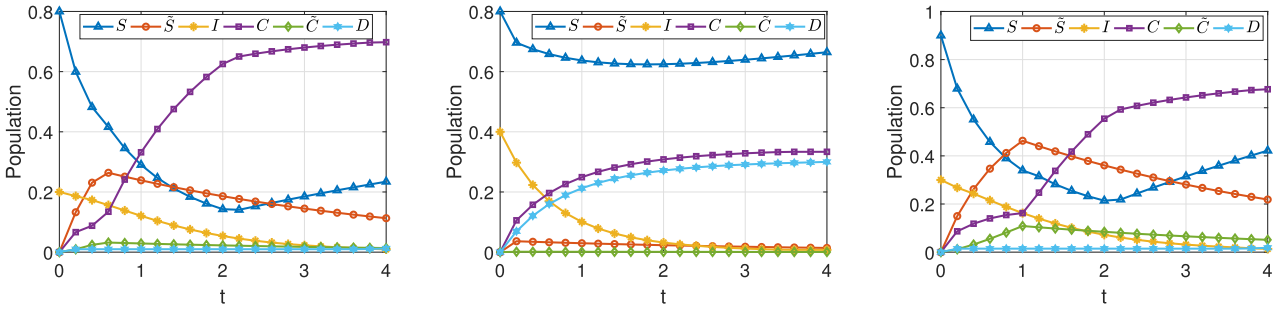
E. Impact of Transmission Range on Non-Cooperation State

In this section, we investigate the impact of transmission range R on the defense strategy ρ. We change the value of R from 1 to 30 with fixed $V_{\max} = 5$ and $q = 0.8$. Fig. 8 shows how many the number of time slots during which the defense strategy is $\rho^k = 1$ for each UE type changes with R. As shown in Fig. 8, when the transmission range R is small (i.e. $R = 1$ to $R = 5$), R has little influence on the defense strategy ρ^k. This is because the infectious UEs have a low value of P^k, and the defender can use same strategy ρ^k to deal with the malware attack. As R increases, the defender puts more UEs into the non-cooperation state. This is because with a larger R, malware has a larger chance of meeting and infecting susceptible UEs. To thwart malware propagation, the defender therefore becomes more conservative in collaborative offloading.

F. Performance Comparison

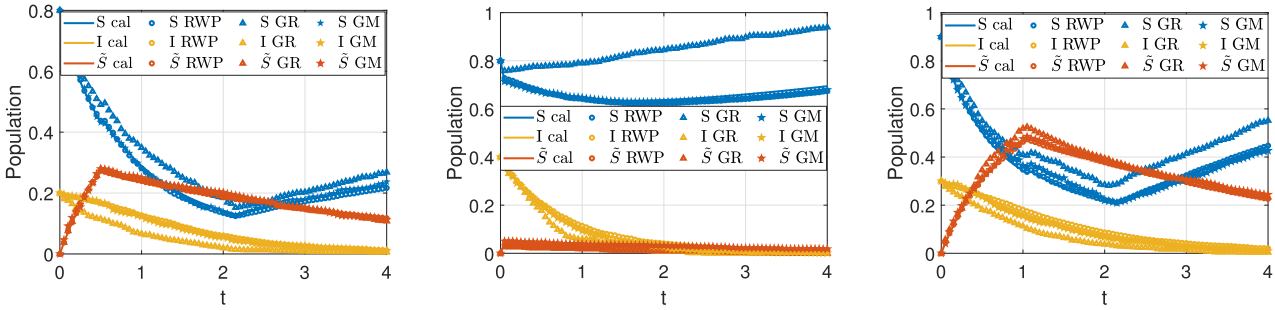
Finally, we compare the performance (in terms of the achievable system utility) of our optimal dynamic strategy with six benchmark strategies:

1) *Static strategies* $\phi = 0, \nu = 1$: the attacker exerts the maximum effort while the defender does nothing.
2) *Static strategies* $\phi = 1, \nu = 0$: the attacker does nothing while the defender exerts the maximum effort.
3) *Static strategies* $\phi = 1, \nu = 1$: both the attacker and the defender exert the maximum effort.



(a) type 1 (b) type 2 (c) type 3

Fig. 6. System evolution.



(a) type 1 (b) type 2 (c) type 3

Fig. 7. System evolution under different mobility models.

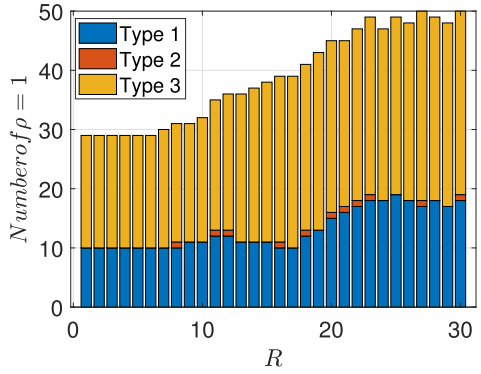


Fig. 8. Impact of transmission range R on non-cooperation population.

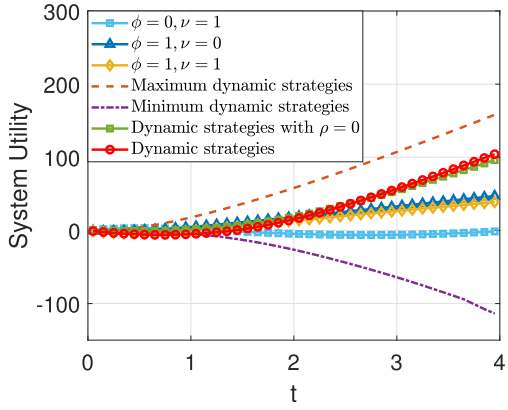


Fig. 9. System utility over time.

4) *Maximum dynamic strategies*: both the attacker and the defender adjust their dynamic strategies to maximize the system utility. This can serve as an upper-bound on the performance of all possible strategies as both the attacker and the defender work together towards a common goal.
5) *Minimum dynamic strategies*: both the attacker and defender adjust their dynamic strategies to minimize the system utility. This can serve as a lower-bound on the performance of all possible strategies.
6) *Dynamic strategy without non-cooperation*: the defender always sets strategies $\rho = 0$.

Fig. 9 demonstrates the total system utility value achieved by various strategies. As can be seen, the maximum dynamic strategy indeed outperforms all other strategies as both the attacker and the defender are working to maximize the utility. However, this strategy is impossible in practice as the attacker and the defender have opposite goals. Our dynamic strategy outperforms the remaining baseline strategies, which significantly beats the intuitive static strategies and also beats the dynamic strategy without considering the non-cooperation option. It is worth noting that the dynamic strategy is barely satisfactory at the beginning (i.e. before $t = 2$) but dramatically improves later (i.e. after $t = 2$). The reason of this result is twofold: (1) at the beginning, the attacker exerts the most effort to infect susceptible UEs and the defender exerts the most effort to patch infectious UEs and hence, the system utility decreases because of the patching cost and the declining population of susceptible UEs. (2) At the same time, the defender also makes many UEs to the non-cooperation states,

which further reduces the population of active UEs. However, at a later time, the dynamic strategy begins to accumulate a higher system utility because the malware has been effectively controlled due to the early effort.

VI. Conclusion

In this paper, we proposed an analytical framework for modeling and understanding the malware propagation in D2D offloading-enabled mobile network with heterogeneous UEs. Based on our model, we showed the existence of an epidemic threshold with respect to the persistence of malware propagation and provided sufficient conditions on the global asymptotically stability of invariant states of our D2D offloading system. Furthermore, we formulated a malware defense differential game, proved the saddle-point equilibrium of this game and derived the optimal dynamic defense and attack strategies. Simulations were performed to validate our model and show the effectiveness of the dynamic strategies. While our model sheds lights on the optimal defense in the D2D offloading system facing epidemic risks, there are still several directions where improvements can be made to make the model richer and more realistic, including periodic re-launched attacks and heterogeneous localized device contact patterns.

References

[1] B.-C. Seet, S. F. Hasan, and P. H.-J. Chong, "Recent advances on cellular D2D communications," MDPI, Basel, Switzerland, 2018.

[2] D. Chatzopoulos, M. Ahmadi, S. Kosta, and P. Hui, "Have you asked your neighbors? A hidden market approach for device-to-device offloading," in *Proc. IEEE 17th Int. Symp. World Wireless, Mobile Multimedia Netw.*, 2016, pp. 1–9.

[3] M. Wang and Z. Yan, "Security in D2D communications: A review," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1, 2015, pp. 1199–1204.

[4] Y. Xu, W. Cui, and M. Peinado, "Controlled-channel attacks: Deterministic side channels for untrusted operating systems," in *Proc. IEEE Symp. Secur. Privacy*, 2015, pp. 640–656.

[5] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott, "Security and privacy in device-to-device (D2D) communication: A review," *IEEE Commun. Surv. Tuts.*, vol. 19, no. 2, pp. 1054–1079, Second Quarter 2017.

[6] R. E. Kopp, "Pontryagin maximum principle," in *Mathematics in Science and Engineering*, vol. 5. Amsterdam, The Netherland: Elsevier, 1962, pp. 255–279.

[7] C. You and K. Huang, "Exploiting non-causal CPU-state information for energy-efficient mobile cooperative computing," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 4104–4117, Jun. 2018.

[8] Y. Tao, C. You, P. Zhang, and K. Huang, "Stochastic control of computation offloading to a helper with a dynamically loaded CPU," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 1247–1262, Feb. 2019.

[9] L. Pu, X. Chen, J. Xu, and X. Fu, "D2D fogging: An energy-efficient and incentive-aware task offloading framework via network-assisted D2D collaboration," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 12, pp. 3887–3901, Dec. 2016.

[10] Y. Wang, S. Wen, Y. Xiang, and W. Zhou, "Modeling the propagation of worms in networks: A survey," *IEEE Commun. Surv. Tut.*, vol. 16, no. 2, pp. 942–960, Second Quarter 2014.

[11] G. Chowell, L. Sattenspiel, S. Bansal, and C. Viboud, "Mathematical models to characterize early epidemic growth: A review," *Phys. Life Rev.*, vol. 18, pp. 66–97, 2016.

[12] K. Li, G. Zhu, Z. Ma, and L. Chen, "Dynamic stability of an siqs epidemic network and its optimal control," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 66, pp. 84–95, 2019.

[13] C. Nowzari, V. M. Preciado, and G. J. Pappas, "Analysis and control of epidemics: A survey of spreading processes on complex networks," *IEEE Control Syst.*, vol. 36, no. 1, pp. 26–46, Feb. 2016.

[14] V. M. Preciado and A. Jadbabaie, "Spectral analysis of virus spreading in random geometric networks," in *Proc. 48th IEEE Conf. Decis. Control*, 2009, pp. 4802–4807.

[15] E. Verriest, F. Delmotte, and M. Egerstedt, "Control of epidemics by vaccination," in *Proc. IEEE Amer. Control Conf.*, 2005, pp. 985–990.

[16] M. Khouzani, S. Sarkar, and E. Altman, "Maximum damage malware attack in mobile wireless networks," *IEEE/ACM Trans. Netw.*, vol. 20, no. 5, pp. 1347–1360, Oct. 2012.

[17] T. Lin *et al.*, "Optimal control of a rumor propagation model with latent period in emergency event," *Adv. Difference Equ.*, vol. 2015, no. 1, 2015, Art. no. 54.

[18] L. Chen and J. Sun, "Global stability and optimal control of an sirs epidemic model on heterogeneous networks," *Phys. A, Statist. Mech. Appl.*, vol. 410, pp. 196–204, 2014.

[19] Z. He, Z. Cai, J. Yu, X. Wang, Y. Sun, and Y. Li, "Cost-efficient strategies for restraining rumor spreading in mobile social networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2789–2800, Mar. 2017.

[20] K. Kandhway and J. Kuri, "Optimal resource allocation over time and degree classes for maximizing information dissemination in social networks," *IEEE/ACM Trans. Netw.*, vol. 24, no. 5, pp. 3204–3217, Oct. 2016.

[21] S. Shen *et al.*, "A non-cooperative non-zero-sum game-based dependability assessment of heterogeneous WSNs with malware diffusion," *J. Netw. Comput. Appl.*, vol. 91, pp. 26–35, 2017.

[22] X.-J. Li, C. Li, and X. Li, "Minimizing social cost of vaccinating network SIS epidemics," *IEEE Trans. Netw. Sci. Eng.*, vol. 5, no. 4, pp. 326–335, Oct.–Dec. 2017.

[23] Y. Hayel and Q. Zhu, "Epidemic protection over heterogeneous networks using evolutionary Poisson games," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 8, pp. 1786–1800, Aug. 2017.

[24] M. Khouzani, S. Sarkar, and E. Altman, "Saddle-point strategies in malware attack," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 1, pp. 31–43, Jan. 2012.

[25] S. Shen, H. Li, R. Han, A. V. Vasilakos, Y. Wang, and Q. Cao, "Differential game-based strategies for preventing malware propagation in wireless sensor networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 11, pp. 1962–1973, Nov. 2014.

[26] J. Xu, L. Chen, K. Liu, and C. Shen, "Designing security-aware incentives for computation offloading via device-to-device communication," *IEEE Trans. Wireless Commun.*, vol. 17, no. 9, pp. 6053–6066, Sep. 2018.

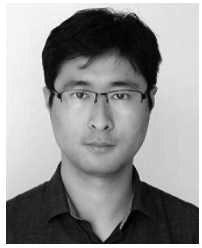
[27] L. Lei, Z. Zhong, C. Lin, and X. Shen, "Operator controlled device-to-device communications in LTE-advanced networks," *IEEE Wireless Commun.*, vol. 19, no. 3, pp. 96–104, Jun. 2012.

[28] L. Chen and J. Sun, "Optimal vaccination and treatment of an epidemic network model," *Phys. Lett. A*, vol. 378, no. 41, pp. 3028–3036, 2014.

[29] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing*. Berlin, Germany: Springer, 1996, pp. 153–181.

[30] F. Bai and A. Helmy, "A survey of mobility models," *Wireless Adhoc Netw.*, vol. 206. p. 147.

Letian Zhang received the B.S. degree in electrical engineering from Shanghai Normal University, Shanghai, China, in 2012 and the M.S. degree in electrical engineering from Shanghai University, Shanghai, China, in 2015. He is currently working toward the Ph.D. degree with the College of Engineering, University of Miami. From 2015 to 2017, he was with ZTE Company as a Software Engineer. His primary research interests include mobile edge computing, game theory, and machine learning for networks.



Jie Xu (S'09–M'15) received the B.S. and M.S. degrees in electronic engineering from Tsinghua University, Beijing, China, in 2008 and 2010, respectively and the Ph.D. degree in electrical engineering from UCLA in 2015. He is an Assistant Professor in Electrical and Computer Engineering Department, University of Miami, Coral Gables, FL, USA. His primary research interests include mobile edge computing, machine learning for networks, and network security.